

CRS Report for Congress

Received through the CRS Web

The National Security Agency: Issues for Congress

Updated January 16, 2001

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

The National Security Agency: Issues for Congress

Summary

The National Security Agency (NSA), one of the largest components of the U.S. Intelligence Community, has reached a major watershed in its history. Responsible for obtaining intelligence from international communications, NSA's efforts are being challenged by the multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states.

NSA's efforts to adjust to the changing geopolitical and technological environment have been strongly encouraged by Congress and reflect a major shift in congressional oversight of the Agency. Although Congress has always approved funding for NSA, for decades routine oversight was limited to a few Members and staff. In the 1970s, congressional investigations of intelligence agencies resulted in greater public attention to NSA and criticism of activities that infringed on the civil liberties of U.S. persons. Subsequently, both the Senate and the House of Representatives established intelligence oversight committees that have closely monitored NSA's operations. The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 to regulate collection by foreign intelligence agencies of the communications of U.S. persons. The end of the Cold War, the expansion of low-cost encryption and the explosion of communications systems led Congress to take a more public profile in overseeing the large and secretive Agency.

Reacting in large measure to congressional concerns, NSA launched two separate management reviews, one by outside experts, the other by longtime Agency officials. Both made strong criticisms of Agency personnel policies, an outmoded organizational structure, and an unwillingness to utilize civilian practices that more effective than those available in-house. The current NSA Director, Lt. General Michael V. Hayden, USAF, has used these analyses to launch a series of major initiatives designed to improve NSA's operations, to attract and reward more qualified people from outside industry, and is developing a major contract for outside support of its non-sensitive Information Technology (IT) functions.

A major renewal effort is underway, but observers believe many challenges lie ahead that will require congressional oversight. Many of the reforms in personnel policies recommended are difficult to implement in a government organization, especially in an extremely tight market for technical specialists. The technical complexities of dealing with widespread and sophisticated encryption as well as the proliferation of communications devices remain to be resolved. NSA is, along with other intelligence agencies, not well-positioned to analyze developments among the assortment of terrorist groups and narcotics smugglers around the world that can seriously affect U.S. interests. NSA has also come under heated criticism in the European Parliament for allegedly collecting, in cooperation with the British, commercial intelligence to benefit U.S. corporations.

Contents

Introduction	1
Roles and Missions: The Growing Influence of Congress	2
Changing Technologies	3
Personnel Matters	5
Diversity and Equal Opportunity Issues	5
Changing Personnel Requirements	6
Charting NSA's Future Direction	7
Director Hayden's Initiatives	8
Elements of Uncertainty	11
Conclusion	13
Appendix A. Congressional Oversight of NSA: A Brief Review	15
Appendix B. Cooperation with Other Countries and the Echelon Controversy .	23

The National Security Agency: Issues for Congress

Introduction

The National Security Agency (NSA), one of the largest components of the U.S. Intelligence Community, has reached a major watershed in its history. Responsible for obtaining intelligence from international communications,¹ NSA's efforts are being challenged by the multiplicity of new types of communications links, by the widespread availability of low-cost encryption systems, and by changes in the international environment in which dangerous security threats can come from small, but well organized, terrorist groups as well as hostile nation states.

NSA was established in 1952 as a highly compartmented secret codebreaking effort undertaken by a handful of military officers and civilians, but the Agency has gradually become an acknowledged government agency responsible for signals intelligence (sigint). This evolution has been in significant measure a result of congressional initiatives. Congress provided the statutory framework for NSA and its activities. Laws have been enacted that carefully prescribe the limits of NSA's electronic surveillance of U.S. persons. Congress has been increasingly inclined to take public notice of problems at NSA and is supporting reforms that are designed to make NSA more effective in current technological and geopolitical environments.

The challenges facing NSA are formidable; a difficult operational environment as well as limitations on spending levels for intelligence call into question the future capabilities of NSA. Public interest in NSA has been heightened in recent months by some members of the European Parliament who allege that the United States and a few other countries are cooperatively engaged in systematic electronic eavesdropping in order to promote the commercial interests of U.S. corporations. This Report will

¹ A primary responsibility of NSA is the collection and analysis of signals intelligence a function that has been described by Director of Central Intelligence George Tenet as "one of the pillars of US intelligence. Along with our other intelligence collection activities, we rely on SIGINT to collect information about the capabilities and intentions of foreign powers, organizations, and persons to support the foreign policy and other national interests of the United States. SIGINT is critical to monitoring terrorist activities, arms control compliance, narcotics trafficking, and the development of chemical and biological weapons and weapons of mass destruction." Statement by Director of Central Intelligence George J. Tenet before the House Permanent Select Committee on Intelligence, April 12, 2000. NSA is also responsible for protecting information systems security of U.S. Government agencies. This is an increasingly important NSA mission that includes the preparation of codes and encoding devices, but the focus of this report will be on the more controversial intelligence collection and analysis mission.

attempt to provide an unclassified description of NSA's evolution, the technical and operational environment that now exists, and indicate some issues that the executive branch and Congress will be facing in coming years.

An unmistakable change affecting NSA has been the openness with which its policies and problems are now discussed both by the Agency's leadership and by congressional oversight committees. Until very recently NSA was the most secretive intelligence agency, more shielded from public scrutiny than the Central Intelligence Agency (CIA). Only the most elliptical references were made in public to the sigint mission, and at one time, NSA employees identified themselves only as working for the Defense Department. In the past few years, however, senior intelligence officials frequently describe NSA's problems and reports accompanying intelligence legislation include extensive commentary on the challenges facing NSA and the approaches encouraged by Congress. These changes were made possible by the absence of a superpower competitor capable of exploiting any inadvertent security slip and by the need to justify intelligence spending at a time when international climate is apparently more benign. These factors removed inhibitions against NSA "going public" and, at the same time, created a political environment that would require public understanding of NSA's mission if the Agency could continue to obtain the funding necessary to update its operations.

Roles and Missions: The Growing Influence of Congress

For decades Congress was content to consider the signals intelligence effort and the organization of NSA primarily as the responsibility of the executive branch. For a quarter century after the end of the Second World War, NSA and the nation's other intelligence agencies undertook their activities with little publicity and with congressional interest limited to a handful of members of armed services and appropriations committees. The intelligence investigations of the 1970s, however, led to well-publicized hearings that placed many secrets, including those of NSA, on the public record. Of greater enduring significance was the establishment of select intelligence committees in both the House of Representatives and the Senate. These committees were granted the authority to conduct oversight over the intelligence activities of the Federal Government, including NSA. They became, along with the appropriations committees, the points of contact between the intelligence agencies and Congress. As a result of the extreme sensitivity of much intelligence information, the two intelligence committees came to act essentially as surrogates for the Congress and the public in regard to intelligence agencies. Until the mid-1990s much of interest of the committees, as reflected in report language and public hearings, centered on the CIA and especially its operations directorate. Sigint activities were undoubtedly matters of congressional concern, but they were very rarely the focus of public attention.²

In recent years, with the end of the Cold War the two intelligence committees have had much more intensive concern with NSA as reflected in more detailed report language on NSA's activities. The extent of oversight is reflected by comments in

² For additional information on congressional oversight of NSA, see Appendix A.

the report on the FY2000 Intelligence Authorization bill (H.R. 1555) by the House intelligence committee:

In the last two Congresses, the committee has been direct in its identification of process and management problems that require attention. The committee believes that NSA management has not yet stepped up to the line. There have been some efforts at reform, but there are still several areas where change is not only needed but is critical for NSA's future.³

Congress has taken a more open interest in NSA at a time when the Agency's roles and missions are facing significant reformulation. Congress has provided guidance for NSA's future direction and has made budgetary allocations based on its sense of appropriate goals, personnel policies, and organizational structure. Most observers believe, moreover, that, given the fluid state of international affairs and information technologies, that further congressional attention is likely as NSA changes to adapt to its new environment.

Changing Technologies

The primary targets of electronic surveillance during the Cold War were the communications of hostile military organizations and governments. Most of such communications were encrypted; in many cases this message traffic could be read only sporadically, if at all (although useful information can often be obtained without actually reading the actual messages). Some communications were carried on land lines that could be intercepted only if they could be physically tapped, inevitably a difficult undertaking. It was, nonetheless, the government and military circuits that provided the most important intelligence of military capabilities, hostile intentions, and diplomatic maneuvers that could place this nation's security at risk. Civilian communications—telegraphs, telephones, facsimile devices, etc.—were usually unencrypted and often sources of valuable information, albeit of secondary priority.

In the past decade, two important trends have combined to change the nature of electronic surveillance efforts. The end of the Cold War meant policymakers and military officials had a wider range of countries that they were concerned with and placed much greater emphasis on “non-state actors”—terrorist groups and narcotics smuggling organizations that have come to be seen as genuine national security threats. These links are not necessarily easy targets given the great expansion in international telephone service that has grown by approximately 18% annually since 1992. Intelligence agencies are faced with profound “needle- in-a-haystack” challenges; it being estimated that in 1997 there were some 82 billion minutes of telephone service worldwide.⁴

³ U.S. Congress, 106th Congress, 1st session, House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2000*, H.Rept. 106-130, Part 1, May 7, 1999, p. 12.

⁴ Linda Blake and Jim Lande, *Trends in the U.S. International Telecommunications Industry* (Washington: Federal Communications Commission, 1999), tables 7,9.

The technologies used in civilian communications circuits have also changed; in the past decade reliance on microwave transmissions (which can be intercepted with relative efficiency) has been increasingly displaced by fiber optic cables.⁵ Fiber optics can carry far more circuits with greater clarity and through longer distances and provides the greater bandwidth necessary for transmitting the enormous quantities of data commonplace in the Internet age. Inevitably, fiber optic transmission present major challenges to electronic surveillance efforts as their contents cannot be readily intercepted, at least without direct access to the cables themselves. The widespread use of fiber optics may also affect requirements for expensive sigint satellites since transmissions over fiber optic cables cannot be intercepted from space-based platforms.⁶

In addition to the widespread use of fiber optic cable, civilian communications have been marked by increased access to high-quality encryption systems formerly available only to governments and militaries. Some systems are available at no cost on the Internet and others can be obtained commercially at minimal expense. This has led to an extensive debate in the United States about the need for export controls on sophisticated encryption systems. Although it is universally acknowledged that commercial encryption systems available throughout the world present major challenges to intelligence (and law enforcement) agencies, U.S. intelligence officials have argued that permitting export of high-quality U.S. systems with associated systems support would greatly extend the capabilities of other governments and hostile groups to protect their communications. After extensive discussions within the executive branch and Congress, steps have been taken to loosen, but not remove, U.S. restrictions on encryption exports.⁷ NSA officials were active in criticizing unrestricted encryption exports and observers suggest that these views, which were shared by many in Congress especially within the intelligence and armed services committees, may have fueled press criticism of NSA.

Changing threats, coupled with the evolving global technological environment, have undoubtedly made NSA's tasks far more difficult. The proliferation of communications throughout the world and the spread of encryption may make electronic surveillance almost impossible. Much equipment acquired for Cold War missions is not effective against new targets. In some cases, NSA must resort to analyses of traffic patterns—who is communicating with whom, when, and how often—to provide information that may not be obtainable through breaking of codes and reading of plaintext.

A major shortcoming was revealed in January 2000 when a software anomaly in the communications infrastructure curtailed NSA's operations for some 72 hours. An

⁵ See Ivan Amato, "Fiber Optics: Communicating at Light Speed," *Washington Post*, November 10, 1999, p. H1; Lee Bruno, "Broadband: To Infinity and Beyond," *Red Herring*, February 2000, p. 170.

⁶ See Jeremy Singer, "Sophisticated Fiber Optics Also Problematic for NSA," *Defense News*, June 12, 2000.

⁷ See Richard M. Nunno, *Encryption Technology: Congressional Issues*, CRS Issue Brief IB96039; Richard A. Best, Jr. and Keith G. Tidball, *The Encryption Debate: Intelligence Aspects*, CRS Report 98-905, November 4, 1998.

intensive and expensive effort was required to restore operations. A subsequent assessment found that the fundamental problem was not technical, but doctrinal and organizational.⁸

Personnel Matters

NSA has employed many highly gifted scientists, engineers, and mathematicians. However, shifting geopolitical concerns and budget reductions required in the early 1990's led to early retirements and fewer newly hired employees. During the same period, the Agency was also required to move towards a personnel structure more closely reflective of national demographics. Simultaneously, a revolution in communications and information technologies was launched in many small, start-up firms whose culture and salary and personnel benefit levels were radically different from those of government agencies. As the extent of these problems became apparent, Congress has provided guidance in several areas.

Diversity and Equal Opportunity Issues

At least since the enactment of the National Security Agency Act of 1959 NSA's personnel policies have been the subject of congressional interest. That Act in essence established a separate personnel system for NSA. By the mid-1980s the House Intelligence Committee became concerned with the relatively small numbers of African-Americans, Hispanics, and women within the NSA workforce. (In 1993, blacks constituted 9% of the total number of NSA employees whereas the national labor force percentage was just over 10; the NSA Hispanic percentage was 1.2, whereas the national average was just over 8; for Asian Americans, the national figure was 2.9, at NSA it was 0.9.)⁹ One congressional initiative included provisions in the FY1987 Intelligence Authorization Act (P.L.99-569) amending the National Security Agency Act to establish an undergraduate training program to facilitate the recruitment of minority high school students with skills in mathematics, computer sciences, engineering and foreign languages. Recruitment efforts were made in colleges with higher concentrations of Hispanic students and efforts were made to ensure equal consideration in promotions. By 1996, NSA had made measurable increases in minority and female representation in the general workforce and in

⁸ See Walter Pincus, "NSA System Crash Raises Hill Worries," *Washington Post*, February 2, 2000, p. 19; Michael V. Hayden, "Background on NSA: History, Oversight, Relevance for Today," *Defense Intelligence Journal*, Summer 2000, p. 31. During this period the British reportedly helped to supply data that NSA could not obtain directly; see Ben MacIntyre, "UK Spied for US as Computer Bug Hit," *Times* (London), April 27, 2000.

⁹ Statement of Vice Admiral J.M. McConnell, USN, Director, National Security Agency/Chief, Central Security Service in U.S. Congress, 103rd Congress, 1st session, House of Representatives, Permanent Select Committee on Intelligence, *Central Intelligence Agency, Defense Intelligence Agency and National Security Agency: Minority Hire, Retentions and Promotions*, Hearing, October 28, 1993, p. 27.

leadership positions.¹⁰ These initiatives were not welcomed by all NSA personnel, with some officials expressing concerns that others would receive preference at their own expense.¹¹ Since the mid-1990s public congressional hearings and published committee reports have not given extensive discussion to diversity issues. Although efforts continue to increase the diversity of NSA's workforce, other personnel issues have complicated hiring and promotion policies.

Changing Personnel Requirements

Since the end of the Cold War, the nature of sigint targets has changed; the sheer quantity of communications has dramatically risen and sophisticated encryption systems are increasingly available throughout the world. These changes in targets and technologies have required a substantially different NSA workforce. Long staffed by civil servants and military personnel who made their whole careers in cryptologic specialities; NSA officials must now be able to shift rapidly among disparate sigint efforts and varying targets. Different skill mixes are required at NSA at a time when technical specialists in communications, computer services, and encryption systems are in high demand throughout the economy. Observers believe that entry- and mid-level government salaries are not equal to opportunities currently available in an especially dynamic sector of the economy; furthermore, workers in technical fields often shift jobs in short periods and it may not be possible to retain them solely on the basis of the career benefits of federal service.¹²

As has been the case with other intelligence agencies, staffing levels at NSA have been reduced during the past decade. Many analysts and others who spent their careers focusing on Soviet and Warsaw Pact issues no longer directly relevant to U.S. security concerns have retired or moved into new specialities. Some media observers suggest, however, that NSA continues to be burdened by an "old guard" of Cold War-era careerists whose talents are not precisely suitable to emerging missions. Although such charges are difficult to document (and may only reflect bureaucratic politics), it is generally acknowledged that NSA will have to adopt an altered personnel structure. FY2001 Intelligence Authorization legislation (passed by both houses, but vetoed by the President because of concerns not directly related to NSA) would provide authority for NSA to offer early retirement and voluntary separation

¹⁰ U.S. Congress, 104th Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Human Resources and Diversity*, Hearing, September 20, 1996, pp. 28-29.

¹¹ U.S. Congress, 103d Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Hiring, Promotion, Retention and Overall Representation of Minorities, Women and Disabled Persons within the Intelligence Community*, Hearing, September 20, 1994, pp. 124-125.

¹² In November 2000 the Office of Personnel Management announced that it was establishing higher rates of basic pay for entry- and mid-level information technology (IT) workers throughout the Federal Government, with net pay increases ranging from 7 to 33%. The IT categories involved include a significant number of positions at NSA. NSA is also preparing to implement a new compensation structure that will use variable pay to recognize and reward achievement. See "NSA Chief Pushes Ahead with Overhaul of Agency's Culture, Operations," *Defense Information and Electronics Report*, October 20, 2000, p. 5.

pay to employees with 20 or 25 years of service (depending on age). This provision was inserted to provide the NSA Director with the opportunity to institute personnel changes that are considered necessary and reflects the intelligence committees view that “the situation at NSA is unique, not only in the enormity of the task of modernization, but also in the direct impact on national security should NSA modernization fail.”¹³

One approach that has been adopted is to increase reliance on contracting out personnel services although security considerations can complicate the use of non-career personnel.¹⁴ In some cases it has been possible to acquire the services of some retired NSA officials who are able to receive the relevant clearances with little delay. In other situations NSA is able to compartmentalize some activities and make use of specialists who do not need access to sensitive information. Some observers warn, however, that contract personnel will tend not to be as committed to the Agency’s missions, and may work subsequently for non-government concerns with an increased possibility of unauthorized sharing of classified information.

Charting NSA’s Future Direction

In recent years, congressional oversight committees have become concerned about the effect of the changed international threat environment and new technologies on NSA’s future effectiveness. The requirement to replace aging satellite systems in particular have placed pressures on intelligence spending across the board; the size and extent of NSA’s budget inevitably meant that it would be subject to close scrutiny. Thus, in 1997 the Senate Select Committee on Intelligence established a Technical Advisory Group (TAG) to review the U.S. sigint effort along with other technical challenges facing the Intelligence Community. The TAG was composed of leading U.S. scientists and experts in technology and intelligence and has made two classified reports on NSA’s capabilities. According to the Senate Committee, the TAG identified serious deficiencies; “as resources have been reduced, the NSA systematically has sacrificed infrastructure modernization in order to meet day-to-day intelligence requirements. Consequently, the organization begins the 21st Century lacking the technological infrastructure and human resources needed even to maintain the status quo, much less meet emerging challenges.”¹⁵ One media account indicates that the TAG’s conclusions were highly critical: “We told them that unless you totally change your intelligence-collection systems you will go deaf,” one involved official [stated]. “You’ve got ten years.” According to the account, the Group

¹³ U.S. Congress, 106th Congress, 2d session, Committee of Conference, *Intelligence Authorization Act for Fiscal Year 2001*, H.Rept. 106-969, October 11, 2000, p. 46.

¹⁴ George Cahlink, “NSA May Outsource 5,000 High-Technology Jobs,” *Defense News*, June 12, 2000, p. 4.

¹⁵ U.S. Congress, 106th Congress, 2d session, Senate, Select Committee on Intelligence, *Authorizing Appropriations for Fiscal Year 2001 for the Intelligence Activities of the United States Government and the Central Intelligence Agency Retirement and Disability System*, S.Rept. 106-279, May 4, 2000, p. 6.

“urged that the agency immediately begin a major reorganization, and start planning for the recruitment of several thousand skilled computer scientists.”¹⁶

According to the Senate report, the TAG also recommended new business procedures and additional resources. The report indicated that the FY2001 authorization bill would likely reflect TAG recommendations, with resources being shifted to long-term infrastructure modernization at the expense of some short-term collection.¹⁷

The House Permanent Select Committee on Intelligence also reached the conclusion in 1998 that “very large changes in the National Security Agency’s culture and method of operations need to take place.”¹⁸ The Committee indicated its approach:

First, the committee is funding and mandating external management reviews. Second, the committee is attempting to infuse fresh thought, needed expertise (especially in systems engineering), and greater fairness by insisting that significant portions of certain categories be contracted out and that outside proposals and expertise be solicited, notably in systems engineering, advanced research and development, and in development activities.... Third, fences have been placed on portions of the budget, with the prospect that a considerable amount of money could be reprogrammed for other [Intelligence Community] needs if NSA does not develop detailed strategic and business planning.¹⁹

The House committee envisioned “a far more radical revision of the budget process than presently contemplated.” Emphasis would be placed on “a new culture in which all team together on a new architecture.”

Director Hayden’s Initiatives

Aware of the challenges facing the Nation’s sigint effort and responsive to congressional concerns, the senior leadership of NSA has been moving to make drastic changes in NSA’s operations and organization. Upon becoming NSA’s director in March 1999 Air Force Lt. General V. Michael Hayden assigned a number of mid-level NSA officials to review the Agency’s organizational structure. Known as the New Enterprise Team, the group recommended a new executive leadership team, the development of strategic business plans, the acquisition of agency wide management information systems, and hiring a financial management officer. A

¹⁶ Seymour M. Hersh, “The Intelligence Gap,” *New Yorker*, December 6, 1999, pp. 62, 64.

¹⁷ Additional background on NSA’s managerial challenges is provided in “NSA Overhauls Corporate Structure in Effort to Improve Operations,” *Inside the Air Force*, June 23, 2000.

¹⁸ U.S. Congress, 105th Congress, 2d session, House of Representatives, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 1999*, H. Rept. 105-508, May 5, 1998, pp. 9-10.

¹⁹ *Ibid.*, p. 10.

separate report by a smaller group of outside experts with experience in the telecommunications industry made similar recommendations.²⁰

The two sets of recommendations reflected a consensus by these advisory groups (and by congressional overseers) that NSA requires more centralized management, that separate divisions that had long enjoyed functional independence need greater coordination to reduce duplicative functions, and that there needs to be a strategic vision of how the Agency is to adapt to changed geopolitical and technological environments. Both reports reflected confidence in the importance of NSA's missions, but both were highly critical of NSA's management and personnel structures. The outside experts concluded: "The most serious issues are leadership, accountability, and empowerment, as evidenced by great dissatisfaction with decision making within the Agency."²¹ The NSA officials noted the Agency's fundamental problems: "lack of governance, lack of leadership, and lack of strategic alignment." Although some specific criticisms reflect the inherent limitations of government agencies in comparison with the civilian telecommunications industry, NSA was urged to take special steps to hold middle managers responsible for personnel decisions. Although NSA has traditionally hired recent college graduates and retained them until retirement, changes in technology, in the international environment, as well as disparities in government and civilian salaries, imply that in the future there may be fixed-term positions and upgraded salary levels for some critical technical specialists.

NSA was also urged to move away from its traditional preference for performing all functions in-house rather than to look for creative ways to find civilian contractors not just as sources of manpower but as "solution providers," and to make hard choices over priorities rather than to make across-the-board budgetary reductions. The outside team of experts urged NSA not only to take advantage of the potential advantages of outsourcing but also to bring in mid- and upper-level managers from successful businesses.

In November 1999, Hayden launched "100 Days of Change"—another series of managerial initiatives responsive to the recommendations of these groups. He subsequently summarized NSA's challenges: "maintaining a strong infrastructure of people and facilities in a time of constrained budgets; accurately forecasting technology trends in the face of an explosion of information systems; and reacting agilely to new technological innovations."²²

With congressional support Hayden has brought in industry experts from civilian firms to develop a comprehensive business plan for the Agency that will enable it to perform in a transformed global information technology arena. An initial step was the

²⁰ Bob Brewin, Daniel Verton, and William Matthews, "NSA Playing IT Catch-Up," *Federal Computer Week*, December 6, 1999, p. 1. The report by NSA officials, New Enterprise Team, *The Director's Work Plan for Change*, October 1, 1990, and the External Team Report, October 22, 1999, were subsequently made available on NSA's Web site [<http://www.nsa.gov>].

²¹ External Team Report, October 22, 1999, p. 4.

²² NSA Press Release, 7 January 2000, *Director of National Security Agency Welcomes Ms. Beverly Wright, Chief Financial Manager*.

appointment of a new chief financial manager from private industry in January 2000. He has also hired a chief information officer, a senior acquisition executive, and created a transformation office. It is hoped that these officials will provide the capability for strategic planning and centralized coordination that NSA has been criticized for not maintaining. In July 2000 it was announced that William Black, Jr., a former NSA official who had retired and found employment in a high-tech consulting firm, Science Applications International Corporation, would be appointed deputy director. Black replaces Barbara McNamara who has been widely blamed in some media accounts²³ as part of an “old guard” that has delayed NSA’s transition to post-Cold War challenges. McNamara has been assigned as head of NSA’s liaison office in London.

In October 2000, further adjustments in NSA’s management structure were announced. General Hayden will serve as Director and Chief Executive Officer and intends to focus on implementing the changes necessary to keep NSA relevant to the needs of the rest of the Government. Deputy Director Black will also serve as Chief Operating Officer and be responsible for day-to-day operations. A new Executive Leadership Team will be created to concentrate on overall strategic planning issues, composed of Hayden, Black, and the deputy directors for operations, information assurance, and technology.²⁴

In June 2000 NSA announced that it intended to contract out “non-mission related” information technology (IT) support—information technology functions that are not part of its core cryptologic efforts.²⁵ A \$4 billion IT contract, to be known as Project Groundbreaker, will be awarded for handling many of the Agency’s extensive and varied requirements for information processing including desktop and workstation computers, email, network operations, software and telephone systems.²⁶ Hayden indicated that NSA divisions traditionally had undertaken much of their own IT work to support their ongoing operations, with inadequate concern for overall financial implications for the entire Agency. He was quoted in one account:

I knew exactly how much activity X cost. I knew when we spent the money, I knew what it cost, I knew when it was appropriated. But we didn’t really have the ability to aggregate all activity Xs and portray them to the agency as, “Hey, by the way, do you realize that is what activity X cost you around the world and do you really want to be spending [this] percentage of your budget on activity X as opposed to activity Y?” We couldn’t do that. We couldn’t pull the thread and

²³ Especially by Hersh, “The Intelligence Gap,” p. 62.

²⁴ “NSA Chief Pushes Ahead with Overhaul,” *Defense Information and Electronics Report*, October 20, 2000, pp. 1,4.

²⁵ For additional background on outsourcing issues, see Valerie Grasso, *Defense Outsourcing: the OMB Circular A-76 Policy*, CRS Report RL30392, April 12, 2000.

²⁶ Cahlink, “NSA May Outsource 5,000 High-Technology Jobs.” The Request for Proposal for Groundbreaker is anticipated in January 2001 with the award of a contract in July 2001.

aggregate what it was we were doing as an enterprise in order to make strategic decisions on direction.²⁷

Hayden realizes that a more centralized system, with much work outsourced to a civilian contractor, may result in having to say “no to legitimate daily operational needs because the system can’t handle it. That is the big change.”²⁸

On November 8, 2000 NSA announced the accomplishment of the initial phase of its new acquisition program and indicated an intention to solicit industry for concept studies for sigint modernization. This initiative is known as Trailblazer and the studies are expected to be undertaken in 2001.

Elements of Uncertainty

Few observers deny that significant structural changes in NSA’s organization are warranted, but some caution that the changes thus far envisioned may not resolve the expected problems. Skeptics note, in particular, that outsourcing is no panacea, that it may mean the loss of experienced personnel with longstanding ties to NSA without necessarily reducing overall costs to the taxpayers. Further, they argue, the necessity of granting sensitive clearances to contractor personnel may increase risks of compromising classified information and processes. All agree that costs of background security investigations will increase.

Other objections may be raised concerning the consolidation of IT functions in a centralized office. The flexibility of individual components to design unique systems may be jeopardized, and the NSA Director has acknowledged that certain legitimate functions may have to be curtailed. Observers note that many of the technological advances in the past decade have been made by decentralized organizations that permit component divisions to establish their own operational practices and develop their own IT solutions without micro-management from a headquarters staff.

The External Team argued that “intelligence targets will continue to be increasingly transnational in nature, and . . . alignment to geographical locations and entities is obsolete.” Although all observers would agree that NSA cannot maintain uniform depths of area expertise for all potential concerns, some suggest that there are areas that will be of intense concern to the U.S. Government for decades to come and dispersing area familiarities acquired over many years would be seriously mistaken.

Congressional observers strongly support the use of NSA’s budget to establish priorities. They do not indicate that they believe NSA has mishandled funds; they do maintain that the Agency has not managed its budget to achieve managerial goals. In 1999 the House Intelligence Committee noted that “In the last two Congresses, the

²⁷ Quoted in “NSA Overhauls Corporate Structure in Effort to Improve Operations,” *Inside the Air Force*, June 23, 2000, p. 1.

²⁸ “NSA Overhauls corporate Structure to Improve Operations.” Also, “NSA to Pursue Government-Industry Partnership for Information Technology Infrastructure Services,” NSA Press Release, June 7, 2000.

committee has been direct in its identification of process and management problems that required attention,” but “NSA management has not yet stepped up to the line.” The committee added that it “looks forward to the opportunities for change that present themselves with the introduction of a new Director of NSA.”²⁹

The Senate Intelligence Committee has urged that the NSA Director should have greater authority over the 70% of cryptologic resources that are currently managed by the military services. The military services operate collection sites, undertake initial analysis, and provide direct support to military commanders. NSA is responsible for tasking their efforts and for final analysis of the data they collect. Since service cryptologic elements support both NSA and military commanders there are inevitably differences over their disposition and responsibilities. Although the Senate Intelligence Committee advocates the NSA Director have “centralized direction across the SIGINT infrastructure as he implements his modernization strategy,”³⁰ some in DOD (and perhaps in Congress as well) would argue, however, that the need to configure sigint resources in direct support of operational commanders would argue against such augmented authorities for the leader of a Washington-area agency.

The House Committee, in reporting its version of the FY2001 Intelligence Authorization Act in May 2000 (H.R. 4392), accepted the need for managerial changes at NSA. Criticizing the traditional independence of NSA’s divisions, the Committee argued that:

Each type of communication—radio, satellite, microwave, cellular, cable—is becoming connected to all the others. Each new type of traffic shows up on every type of communication. Unfortunately, as the global network has become more integrated, NSA’s culture has evolved so that is seemingly incapable of responding in an integrated fashion.

The House Committee argued that NSA must, as a result, “prepare itself for complex, prioritized, carefully timed and integrated systems acquisitions that, in aggregate, rival the complexity of programs commonly managed by the NRO, the Defense Department, and commercial industry.”³¹

The House Intelligence Committee’s recommendations for significant shifts in NSA’s budget have not yet been accepted. DOD urged that the changes not be approved pending a review of the results of Hayden’s initial reorganization efforts.³² In particular, DOD, with support by the Senate Armed Services Committee, views with concern any efforts to give the DCI influence over NSA that would detract from

²⁹ H.Rept. 106-130, pp. 12-13.

³⁰ S.Rept. 106-279, p. 7.

³¹ U.S. Congress, House of Representatives, 106th Congress, 2d session, Permanent Select Committee on Intelligence, *Intelligence Authorization Act for Fiscal Year 2001*, H.Rept. 106-620, p. 16.

³² Letter from the Chairman of the Joint Chiefs of Staff and the Secretary of Defense to Chairman, Senate Armed Services Committee, reprinted in U.S. Congress, 106th Congress, 2d session, Senate, Committee on Armed Services, *Intelligence Authorization Act for FY2001*, S.Rept. 106-325, pp. 8-9.

that of the Secretary of Defense. These separate approaches may not easily be reconciled.

A major issue related to sigint in the post-Cold War environment is the erosion of distinctions between foreign and domestic threats. For example, an attack from outside the borders of the country through cyberspace could result in major damage to U.S. institutions, but responsibilities for monitoring potential threats are complex and in some ways ill-defined. Constitutional principles and statutes sharply distinguish between information gathering by foreign intelligence and domestic law enforcement agencies and efforts to involve NSA in surveillance of U.S. persons have been sharply restricted. Various administrative arrangements have been made to facilitate cooperation between NSA and the FBI and other law enforcement agencies in gathering information on threats with both foreign and domestic components, but many uncertainties remain. Many observers strongly oppose the use in court cases of information derived from sigint provided by NSA at the same time, sigint specialists are highly reluctant to see NSA diverted from its foreign intelligence missions to tasks that may risk involvement in domestic controversies. Congress, included in the FY2000 Intelligence Authorization bill (H.R. 4392, section 606) a requirement for a report from the Attorney General regarding actions taken in regard to the dissemination of intelligence information within the Justice Department. (This provision replaced an earlier version that would have required the establishment of procedures to accomplish this dissemination.)³³

NSA and counterpart agencies in a number of other countries, especially Great Britain, have come under much criticism in the European Parliament for allegedly monitoring private communications of non-U.S. businessmen in a coordinated electronic surveillance effort known as Echelon in order to support domestic corporations. Some critics go further and charge that NSA's activities represent a constant threat to civil liberties of foreigners and U.S. persons as well. Though NSA has reassured congressional oversight committees that the Agency complies strictly with U.S. law, these controversies will undoubtedly continue.³⁴

Conclusion

The National Security Act establishes sigint as a recognized function of the U.S. Government and requires that it is usually to be carried out by NSA. The U.S. Government thus has accepted responsibility for electronic surveillance activities that are condemned (but not necessarily eschewed) by some foreign countries. Although some specialists in international law argue that electronic surveillance is inherently illegal, U.S. officials contend, based on constitutional responsibilities, statutes, and long-established practice, that electronic surveillance related to national security and

³³ See Richard A. Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, CRS Report RL30252, July 2, 1999; also, J.M. McConnell, "The Future of SIGINT: Opportunities and Challenges in the Information Age," *Defense Intelligence Journal*, Summer 2000, especially pp. 46-47.

³⁴ For further information, see Appendix B.

preventing terrorism and international narcotics smuggling is a legitimate function of the U.S. government. Unlike some foreign countries, the U.S. has not asserted a right to conduct electronic surveillance to support its “economic well-being.”

Managing this effort in a changing geopolitical and technological environment, according to knowledgeable observers and congressional overseers, requires that NSA’s organization and operations be substantially altered. This process is currently underway to strengthen the NSA Director’s role in managing the Agency, but many uncertainties remain that will determine NSA’s future. No national security official can confidently predict what collection priorities will exist in five years time, nor can the equipment acquisition priorities be firmly projected very far into the future. With congressional encouragement, the current leadership of NSA is drawing increasingly on talent available in the civilian community to offset the difficulties involved in retaining talented technological experts in a very tight sector of the labor market. This effort may not result in the stable, loyal workforce that, in the past, led to NSA’s gradual successes against Cold War targets. Some observers also believe that NSA will ultimately require significant budgetary increases at a time when there is a determination to restrict overall government spending.

The future success of NSA is by no means guaranteed. The current NSA Director’s managerial initiatives and the move to use outside contractors have widespread support, but these efforts may not achieve all their intended goals. NSA may not be adaptable to radically changing developments in international telecommunications and the bewildering emergence of terrorist groups previously unheard of. The wider public may come to view NSA’s activities as inherent threats to privacy that outweigh the value of information acquired. Attention will be paid to the costs and benefits of allocating additional funds to NSA at a time when there are sure to be competing demands.

The current level of congressional concern with NSA is unlikely to diminish. Observers expect that, in the face of attacks on NSA by some in the media and by a number of European parliamentarians, members of Congress will be asked to defend or criticize not only NSA’s operations, but also its statutory roles and missions. Funding for NSA’s efforts to adapt to altered geopolitical and technological environments will have to be balanced against other competing needs. To a much greater extent than in the past, observers expect that Congress will continue to involve itself in internal changes in the Agency designed to acquire technological capabilities to acquire information at a time when the volume of communications is expanding exponentially, and access is greatly complicated by the spread of sophisticated encryption systems.

Appendix A. Congressional Oversight of NSA: A Brief Review

Codemaking and signals intelligence (sigint) have long been functions of governments and military organizations.³⁵ Although the United States gave less attention to codemaking and codebreaking than the major European powers, U.S. forces during World War I established a fairly extensive military sigint effort. In the 1920s and 1930s, the services maintained a small sigint effort and, for a time, the State Department collaborated with the Army in operating an American “Black Chamber” that attempted, with limited success, to intercept and decrypt foreign diplomatic communications. By the time the United States entered World War II, U.S. codebreakers were able to decrypt some codes of Japan, Germany, and other foreign countries. Success in breaking Japanese diplomatic codes, achieved through “the exercise of the greatest ingenuity and utmost resourcefulness” was acknowledged publicly after the end of the war in the congressional report regarding the attack on Pearl Harbor.³⁶

During the course of World War II, sigint efforts proved to be exceptionally valuable especially in regard to acquiring military information. The crucial victory at Midway in June 1942 that halted Japan’s advance in the Pacific was gained through sigint. The Allies’ ability to keep supplies flowing across the North Atlantic depended on limiting U-boat attacks; this too was accomplished through good sigint. Some observers have concluded that sigint enabled the Allies to end the war at least a year earlier than would otherwise have been possible.

During World War II, cooperation with the British in sigint collection and analysis proved very fruitful. Although both countries were initially reluctant to share their codebreaking secrets, they gradually came to appreciate the advantages of sharing both collection and analysis. Anglo-American cooperation did not end with the conclusion of hostilities in 1945, but actually expanded with the beginning of the Cold War and the expansion of U.S. security interests throughout the world. The relationship with the British would eventually encompass the Canadians, Australians, and, to a lesser extent, the New Zealanders.

³⁵ For background, see David Kahn, *The Codebreakers: the Story of Secret Writing* (London: Weidenfeld and Nicolson, 1967). The first substantial description of NSA’s activities was James Bamford, *The Puzzle Palace: A Report on America’s Most Secret Agency* (Boston: Houghton Mifflin, 1982). The creation of NSA is described in a 1952 document known as the Brownell Report that was later declassified and published as George A. Brownell, *The Origins and Development of the National Security Agency* (Laguna Hills, CA: Aegean Park Press, 1981).

³⁶ See U.S. Congress, 79th Congress, 2nd session, Joint Committee on the Investigation of the Pearl Harbor Attack, *Investigation of the Pearl Harbor Attack*, Joint Committee Print, 1946, p. 179. Congressional pressure led the Truman Administration to authorize public release of information on the prewar sigint effort against Japan and the ensuing report included detailed discussion of sigint efforts prior to the Japanese attack since they were part of a major controversy surrounding the extent of preparedness at Pearl Harbor in 1941.

After the War, the Army and the Navy, and subsequently the newly independent Air Force all continued sigint collection. An effort was made to coordinate the services' sigint efforts in a single organization known as the Armed Forces Security Agency established by the Secretary of Defense in 1949. Coordination problems were not, however, resolved until October 1952 when President Truman established the National Security Agency in an effort to provide a more effective structure for coordinating signals intelligence activities. Truman had determined that the sigint function was "national," that it would serve civilian policymakers in the State Department and the White House as well as the military. This action was taken in a secret memorandum that was not made public at the time.

NSA became the U.S. focal point of a global sigint effort. Signals are collected at field stations throughout the world, most of which operated by the military services. Some initial processing and analysis may have been performed at the collection site, but in general the "take" is forwarded to NSA, which moved its headquarters from Arlington, Virginia to Fort Meade, Maryland in 1957. After decryption and analysis, the resultant data is provided to "all-source" intelligence agencies such as the CIA or the Defense Intelligence Agency (DIA). NSA has always been staffed by a combination of civil servants and active duty military personnel, but the Agency also provides operational guidance to sigint collection stations maintained by the cryptologic elements of the military services (collectively described as the Central Security Service (CSS)).

During the Cold War, NSA's operations, along with those of allied countries) were primarily directed at the Soviet Union, its Warsaw Pact allies, and Communist China. Massive efforts were made to collect sigint dealing with military threats to the U.S. and its allies. In addition to sigint provided to national-level decision makers, tactical sigint collection, analysis and reporting was incorporated in military operations, including those occurring in the Korean and Vietnam Wars.

For many years NSA's efforts did not receive much public scrutiny. Congressional oversight was conducted by small sub-committees of armed services and appropriations committees without public hearings. The first major legislation dealing directly with NSA was the National Security Agency Act of 1959 (P.L. 86-36). This Act did not describe the functions of NSA, but dealt with "housekeeping" matters such as pay and allowances, training, property acquisition, and leasing. It exempted NSA from the requirement to provide detailed information regarding organizational and functional matters to the Civil Service Commission (the predecessor of the Office of Personnel Management). These authorities are, in general, similar to those exercised by the Director of Central Intelligence (DCI) in regard to the CIA. The act has been amended from time to time and serves as the statutory basis for NSA's personnel policies that derive from its unique mission, including special pay and allowances for overseas travel, professional and foreign language training, and property leasing, and use of the NSA.

An exception to the practice of congressional reticence regarding NSA was a report on a widely publicized defection in 1960 of two NSA employees to the Soviet

Union.³⁷ The committee criticized personnel security procedures as shockingly lax and in part as a result of congressional criticism of the handling of the Mitchell/Martin case DOD tightened the security practices at NSA to ensure that background investigations were completed prior to granting access to cryptologic materials. In 1964 P.L. 88-290 (known as Title III of the Internal Security Act of 1950) was enacted to establish requirements for security investigations for persons working at NSA. Observers note that it was an early reflection of the importance of congressional oversight. It gave the NSA Director authority to terminate the employment of NSA personnel “whenever he considers that action to be in the best interest of the United States.” Such actions can be taken notwithstanding usual civil service procedures for personnel actions. In 1996 these provisions were superseded by enactment of the FY1997 National Defense Authorization Act (P.L. 104-201, sections 1631-1635) which established intelligence personnel policies for the entire Defense Department, including authority to terminate employees “in the interests of the United States.” Appeals of decisions to terminate can only be made to the Secretary of Defense.³⁸

In the mid-1970s, public concerns that U.S. intelligence agencies were spying on domestic groups opposed to the Vietnam War led to hearings by select committees in both chambers.³⁹ Interest in NSA centered on “watch lists” that had been maintained to collect communications of U.S. citizens who were suspected of ties to hostile foreign countries and groups.⁴⁰ There was also interest in a project, known as Shamrock, by which copies of international telegrams were provided to NSA on a daily basis by three telegraph companies. These practices had been terminated by the early 1970's, but Members of Congress considered that the Agency should be held accountable for them.⁴¹ (The desire to bring such practices under the constraints of statutory law contributed to passage of the Foreign Intelligence Surveillance Act of 1978.)

During the hearings conducted by the Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities (known as the Church Committee after its chairman, Senator Frank Church), for the first time a Director of NSA testified in open session to give a public overview of NSA's

³⁷ U.S. Congress, 87th Congress, 2d session, House of Representatives, Committee on Un-American Activities, *Security Practices in the National Security Agency (Defection of Bernon F. Mitchell and William H. Martin)*, Report [Committee Print], August 13, 1962.

³⁸ See General Accounting Office, *Intelligence Agencies: Personnel Practices at CIA, NSA, and DIA Compared with those of Other Agencies*, GAO/NSIAD-96-6, March 1996.

³⁹ See Loch K. Johnson, *A Season of Inquiry: Congress and Intelligence* (Chicago: Dorsey Press, 1988).

⁴⁰ See Morton H. Halperin, *The Lawless State: the Crimes of the U.S. Intelligence Agencies* (New York: Penguin, 1976).

⁴¹ See U.S. Congress, 94th Congress, 2d session, Senate, Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans*, Book III, 1976, pp. 765-776. The congressional investigation of Shamrock is described by a participant, L. Britt Snider, “Unlucky Shamrock: Recollections from the Church Committee’s Investigation of NSA,” *Studies in Intelligence*, Winter 1999-2000.

responsibilities. Lt. General Lew Allen, Jr., citing the statutory and other authorities under which NSA carried out its responsibilities, stated:

This mission of NSA is directed to foreign intelligence, obtained from foreign electrical communications and also from other foreign signals such as radars. Signals are intercepted by many techniques and processed, sorted and analyzed by procedures which reject inappropriate or unnecessary signals. The foreign intelligence derived from these signals is then reported to various agencies of the government in response to their approved requirements for foreign intelligence.⁴²

Allen also explained in some detail the practice of establishing “watch lists” by which “words, including individual names, subjects, locations, etc.” could be identified within a stream of communications to separate useful information from the vast quantities of chatter. Particular attention was paid to retrieving information relating to terrorism, narcotics, and—a particular concern of the Johnson and Nixon Administrations—foreign influences on domestic groups suspected of fomenting civil disturbances in the U.S. in protest against the U.S. role in the Vietnam war.

Allen indicated that, pursuant to presidential direction, the Secretary of Defense had established NSA in accordance with his statutory authorities. He noted further that “for the past 22 years [i.e., since circa 1953], Congress has annually appropriated funds for the operation of the NSA, following hearings before the Armed Services and Appropriations Committees of both Houses of Congress in which extensive briefings of the NSA’s signals intelligence mission have been conducted.”⁴³

The Church Committee concluded:

The National Security Agency is one of the largest and most technically oriented components of the United States intelligence community. Its basic function is collecting and processing foreign communications and signals for intelligence purposes. NSA is also responsible for creating and supervising the cryptography of all United States Government agencies, and has a special responsibility for supervising the military services’ cryptologic agencies. Another major responsibility is protecting the security of American communications.

The Committee regards these functions as vital to American security. NSA’s capability to perform these functions must be preserved. The Committee notes that despite the fact that NSA has been in existence for several decades, NSA still lacks a legislative charter. Moreover, in its extensive investigation, the Committee has identified intelligence community abuses in levying requirements on NSA and abuses by NSA itself in carrying out its functions. These abuses are detailed in the domestic portion of the Committee report. The Committee finds that there is a compelling need for an NSA charter to spell out limitations which will protect

⁴² Testimony of Lt. Gen. Lew. Allen, Jr., Director, National Security Agency in U.S. Congress, 94th Congress, 1st session, Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Hearings, vol 5. *The National Security Agency and Fourth Amendment Rights*, 1976, p. 17.

⁴³ *Ibid.*, p. 8.

individual constitutional rights without impairing NSA's necessary foreign intelligence mission.⁴⁴

Thus, even a committee widely perceived as antagonistic to intelligence agencies concluded that NSA's sigint mission is "vital to American security." It urged, however, a better statutory framework for the Agency and an enhanced role for congressional oversight to ensure that NSA was not misused in ways that would undermine American liberties.

The complete final report of the House Select Committee on Intelligence (known as the Pike Committee) was never made public, but its published recommendations also included a proposal that the existence of NSA be recognized by specific legislation, that such legislation provide for civilian control of NSA, and that the role of NSA with reference to the monitoring of communications of Americans be defined.⁴⁵

Many of the most important statutory provisions relating to NSA were enacted in the wake of these congressional investigations. Congress passed the Foreign Intelligence Surveillance Act of 1978 (FISA) (50 USC 1801) which establishes procedures for electronic surveillance in the United States for foreign intelligence purposes.⁴⁶ It provides that the Attorney General may authorize surveillance in situations wherein the target is communications of foreign powers; in cases in which communications of U.S. persons might be acquired, then approval of a court, created pursuant to the FISA, would be required. Information acquired in accordance with FISA provisions is to be used for foreign intelligence purposes (even though in recent years Congress has expanded FISA to permit use of some types of information acquired under its provisions to be used for law enforcement purposes in certain circumstances). FISA, in essence, ensures that foreign intelligence electronic surveillance operations within the United States are conducted in accordance with statutory authorities and with supervision by the Justice Department (and with oversight by Congress).

Although in the Pearl Harbor investigations, the U.S. Government officially revealed its prewar sigint efforts, ongoing sigint activities had not been acknowledged. FISA provided authority in U.S. statutory law for electronic surveillance activities to be conducted for foreign intelligence (rather than law enforcement) purposes. In enacting the statute the United States Government accepted responsibility for NSA's activities no matter how they might be regarded in other countries. FISA does of course provide ample warning to foreign countries and foreign groups that the U.S. undertakes electronic surveillance when it perceives it necessary. While the argument

⁴⁴ U.S. Congress, 94th Congress, 2d session, Senate, Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Foreign and Military Intelligence, Book I*, Final Report, S.Rept. 94-755, April 26, 1976, p. 464.

⁴⁵ U.S. Congress, 94th Congress, 2d session, House of Representatives, Select Committee on Intelligence, *Recommendations of the Final Report of the House Select Committee on Intelligence*, H.Rept. 94-833, February 11, 1976, p. 3.

⁴⁶ See Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework for Electronic Surveillance*, CRS Report RL30465, May 17, 2000.

was made that such activities are best undertaken without formal legal authorization and without the Government's accepting responsibility for them, Congress specifically rejected that argument in the belief that intelligence activities, including electronic surveillance, are necessary to protect the national security and that the U.S. Intelligence Community should be subject to law and to oversight by Congress.

In addition to FISA, there were also efforts to establish a "legislative charter" for the agencies of the Intelligence Community, including NSA. Testifying in February 1980, the then Director of NSA, Vice Admiral Bobby R. Inman, supported charter legislation, noting that "while the Agency has been provided with significant Congressional guidance and protection with respect to the information and products produced by the Agency, there was little Congressional guidance on the functions and responsibilities of the Agency and few Congressionally provided statutory tools to be used to perform those functions."⁴⁷ Charter legislation for the entire Intelligence Community became very complex and ultimately was a victim of partisan disputes in the late 1970s.⁴⁸ It was not until 1992 that the National Security Act was amended to provide a functional charter for NSA.⁴⁹ The Act now gives the Secretary of Defense the responsibility to ensure:

through the National Security Agency (except as otherwise directed by the President or the National Security Council), the continued operation of an effective unified organization for the conduct of signals intelligence activities and shall ensure that the product is disseminated in a timely manner to authorized recipients....

Guidance for NSA's activities has been further detailed in a series of executive orders.⁵⁰ E.O. 12333, signed by President Reagan on December 4, 1981 after extensive consultation with Congress, and still in effect, tasks the Secretary of Defense with responsibilities for NSA including:

- (1) Establishment and operation of an effective unified organization for signals intelligence activities, except for the delegation of operational control over certain operations that are conducted through other elements of the Intelligence Community. No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense;
- (2) Control of signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders;

⁴⁷ Testimony of B.R. Inman, Vice Admiral, U.S. Navy and Director of National Security Agency, U.S. Congress, 96th Congress, 2d session, Senate, Select Committee on Intelligence, *National Intelligence Act of 1980*, Hearings, 1980, p. 67.

⁴⁸ See John M. Oseth, *Regulating U.S. Intelligence Operations: A Study in Definition of the National Interest* (Lexington, KY: University Press of Kentucky, 1985).

⁴⁹ By the Intelligence Authorization Act for FY1993 (P.L. 102-496, section 705).

⁵⁰ The first, E.O. 11905, was issued by President Ford on February 18, 1976; the second, E.O. 12036, was issued by President Carter on January 24, 1978.

- (3) Collection of signals intelligence information for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;
- (4) Processing of signals intelligence data for national foreign intelligence purposes in accordance with guidance from the Director of Central Intelligence;
- (5) Dissemination of signals intelligence information for national foreign intelligence purposes to authorized elements of the Government, including the military services, in accordance with guidance from the Director of Central Intelligence;
- (6) Collection, processing and dissemination of signals intelligence information for counterintelligence purposes;
- (7) Provision of signals intelligence support for the conduct of military operations in accordance with tasking, priorities, and standards of timeliness assigned by the Secretary of Defense. If provisions of such support requires use of national collection systems, these systems will be tasked within existing guidance from the Director of Central Intelligence.
- (8) Executing the responsibilities of the Secretary of Defense as executive agent for the communications security of the United States Government;
- (9) Conduct of research and development to meet the needs of the United States for signals intelligence and communications security;
- (10) Protection of the security of its installations, activities, property, information, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the NSA as are necessary;
- (11) Prescribing, within its field or authorized operations, security regulations covering operating practices, including the transmission, handling and distribution of signals intelligence and communications security material within and among the elements under control of the Director of NSA, and exercising the necessary supervisory control to ensure compliance with the regulations;
- (12) Conduct of foreign cryptologic liaison relationships, with liaison for intelligence purposes conducted in accordance with policies formulated by the Director of Central Intelligence; and
- (13) Conduct of such administrative and technical support activities within and outside the United States as are necessary to perform the functions described in sections (1) through (12) above, including procurement.

As noted above, in 1976 the Pike Committee urged civilian leadership for NSA. NSA has always been headed by military officers, but they have served under the direction of both the civilian Secretary of Defense and the (usually) civilian Director of Central Intelligence. In accordance with subsequent amendments to the National Security Act, Directors of NSA are now appointed by the President upon the recommendation of the Secretary of Defense with the concurrence of the DCI (although a recommendation can be submitted without the DCI's concurrence if the

fact of non-concurrence is stated). In recent years, few observers express concerns about the NSA Director being a serving officer.

The amended National Security Act also provides that the DCI develops budgets for the annual National Foreign Intelligence Program which includes NSA. The DCI also establishes the requirements and priorities that govern the collection of national intelligence. These provisions provide authority for the DCI to oversee NSA's budget and operations. There are, however, multiple occasions for differences between the roles of the Secretary of Defense and the DCI. The Defense Secretary is inevitably more focused on aligning NSA closely with the operating forces of DOD and tends to emphasize collection of direct interest to military commanders. The DCI, for his part, tends to see NSA as one component of an interagency effort to gather intelligence for senior policymakers in Washington; he approves collection and analysis priorities that reflect their requirements. These respective responsibilities are well understood; defense and intelligence staffs attempt to make adjustments to accommodate differing requirements within budgetary constraints. Any major reorganization or redirection of efforts, however, that could affect NSA's ability to support either national policymakers or military commanders would be sure to generate criticism from one quarter or another.

The Pike and Church Committees also laid the groundwork for permanent intelligence committees. Subsequent to the establishment of the committees (the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence) in 1976-1977, Members and staff have regularly reviewed NSA programs and adjusted budgetary priorities with almost all hearings being conducted in closed sessions. NSA spending (along with the cryptologic activities of the services and other agencies) is authorized in annual intelligence authorization laws with funding levels indicated only in classified annexes. The two armed services committees also have oversight of most intelligence programs since they involved Defense Department assets.

Appendix B. Cooperation with Other Countries and the Echelon Controversy⁵¹

Although sigint collection and analysis are among the most sensitive activities undertaken by the U.S. Government, close cooperation in these efforts is maintained with several other countries—principally, but not limited to, the United Kingdom, Canada, Australia, and New Zealand. These relationships began during the Second World War when agreements to share signals intelligence were made between the military services of the United States and Great Britain, with separate arrangements made with other Commonwealth countries. This cooperation was widely considered by senior military leaders at the time, and by historians subsequently, with having significantly reduced the amount of time needed to defeat Nazi Germany and Japan as well as the number of Allied casualties. Although both the United States and Great Britain tackled various communications links of the Japanese and Germans (along with those of other countries), arrangements were worked out whereby the American effort was concentrated on the Japanese and the British on the Germans. The division of labor reflected resource limitations—especially among skilled cryptologists—and possession of geographical sites from which enemy transmissions could be intercepted.

With the end of hostilities in 1945, both British and American intelligence officials were reluctant to terminate a highly productive cooperative arrangement. There was continued military cooperation between the two countries in occupation duties in various areas and, when the Soviet Union began to be considered a threat to both countries, intelligence cooperation continued. Cooperation with Canada was considered essential in view of potential Soviet military activities originating in Arctic regions. Formal arrangements to cooperate in collecting and analyzing sigint were made by the two countries (and others) given shared geostrategic interests and limited resources that did not permit expansive unilateral efforts. These agreements were conducted in great secrecy at the time and remain largely classified a half-century later.⁵²

The sigint relationship with the British and other Commonwealth countries has attracted criticism from a number of sources over the years.⁵³ To an extent a close intelligence relationships arguably predispose military and political leaders to

⁵¹ See also Richard A. Best, Jr., *Project Echelon: U.S. Electronic Surveillance Efforts*, CRS Report RS20444, Updated March 2, 2000.

⁵² Post-World War II sigint cooperation with the British was authorized by President Truman as early as September 1945 in approving a recommendation by the Secretaries of State, War, and the Navy. See Christopher Andrew, “The Making of the Anglo-American SIGINT Alliance,” in Hayden B. Peake and Samuel Halpern, eds., *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer* (Washington: NIBC Press, 1994), pp. 104-105; also, Bradley F. Smith, *The Ultra-Magic Deals and the Most Secret Special Relationship* (Novato, CA: Presidio Press, 1993); Stephen Budiansky, “The Difficult Beginnings of US-British Codebreaking Cooperation,” *Intelligence and National Security*, Summer 2000.

⁵³ See, for instance, Duncan Campbell, *The Unsinkable Aircraft Carrier: American Military Power in Britain* (London: Michael Joseph, 1984).

coordinated policies. Some observers object to international agreements made without the formal advice and consent of the U.S. Senate. The secret relationships have been criticized by observers in the U.S., Britain, Australia and elsewhere who oppose international entanglements. Some observers from European Union countries express concern that sigint cooperation among the “Anglo-Saxons” might work against their own economic interests.

Supporters of the such relationships with other countries point to the advantages in shared efforts that conserve intelligence resources. The United States, Britain, Canada, Australia, and New Zealand often have common policies on important international issues, but the existence of close intelligence ties has not precluded different policies (or even, as at Suez in 1956, opposing policies) when national leaders felt them necessary. In the post-Cold War environment, observers believe that sigint cooperation with a number of friendly countries maximizes opportunities to obtain information regarding disparate regional threats from terrorist groups, narcotics traffickers, and dealers in nuclear and other substances used in making weapons of mass destruction.

NSA has long been the target of criticism from those who view intelligence agencies as inevitable threats to civil liberties. In general, however, the Agency’s low public profile and the esoteric nature of its work attracted less attention than the more dramatic covert actions undertaken by the CIA. In the past few years, however, reports prepared under the auspices of the Directorate-General for Research of the European Parliament have described U.S. electronic surveillance efforts. The studies, known as Scientific and Technological Options Assessments (STOA), are prepared by contractors and not by European Parliament’s official staff. A series of these reports have severely criticized NSA, charging it with working together with sigint organizations of the United Kingdom, Canada, Australia, and New Zealand to gather commercial communications and providing the intercepts to U.S. business interests to give them advantages over foreign firms.⁵⁴

The criticisms of NSA by these reports have been echoed by media commentary. One account claims that

It is the new Cold War. The United States intelligence agencies, facing downsizing after the fall of the Berlin wall, have found themselves a new role spying on foreign firms to help American business in global markets.

Echelon is part of a British and American-run world-wide spy system that can “suck up” phone calls, faxes and e-mails sent by satellite. America’s intelligence agencies have been able to intercept these vital private communications, often between foreign governments and European businesses, to help the US win major contracts.⁵⁵

⁵⁴ See especially *Interception Capabilities: Report to the Director General for Research of the European Parliament*, Scientific and Technical Options Assessment Programme Office, European Parliament, April 1999.

⁵⁵ Duncan Campbell and Paul Lashmar, “The New Cold War: How America Spies on Us for
(continued...) ”

Some media accounts state that this entire cooperative endeavor has the codename Project Echelon; others believe that Echelon refers only to the process by which computers operated by cooperating sigint agencies sift through many thousands of intercepts for ones containing pre-programmed key words.⁵⁶

U.S. intelligence officials have responded to these charges by describing the statutory framework under which NSA operates and the oversight mechanisms in place in both the Executive and Legislative Branches. There have been categorical denials that intelligence is passed to U.S. companies to provide them commercial advantages although it is freely acknowledged that sigint is used to provide the U.S. Government with information about bribery and other illegal practices of foreign firms and that this information has been used as the basis for diplomatic complaints.⁵⁷

NSA has successfully persuaded the congressional leadership that it faithfully and responsibly conducts its electronic surveillance activities in accordance with law and relevant executive orders. Section 309 of the Intelligence Authorization Act for FY2000 (P.L. 106-120) required that the Director of NSA submit a report (to be prepared jointly by the Director of NSA, the DCI, and the Attorney General) providing a detailed analysis of the legal standards used in conducting signals intelligence activities, including electronic surveillance. The report was submitted in February 2000 and set forth the legal bases for NSA's activities, emphasizing its commitment to respect the privacy rights of U.S. persons. In a public hearing to discuss the report, Representative Goss, Chairman of the House Intelligence Committee, concluded that "our safeguards are in place and are working."⁵⁸

Most U.S. observers give credence to the official U.S. position, especially given the absence of evidence that U.S. companies are pressuring the Government for help in learning about foreign technologies. Observers suggest, in addition, that any U.S. intelligence assistance to a U.S. firm in winning a foreign contract would provoke strong criticism by a disadvantaged U.S. competitor.⁵⁹ Former DCI R. James

⁵⁵ (...continued)

its Oldest Friend—the Dollar," *Independent* (London), July 2, 2000. Campbell and Lashmar detail instances in which the U.S. Government complained to foreign countries that European firms were attempting to bribe their officials and, as a result, the contracts ultimately went to U.S. firms. They quote others as maintaining that U.S. officials pass intelligence information directly to U.S. corporations.

⁵⁶ See Jeffrey Richelson, "Desperately Seeking Signals," *Bulletin of Atomic Scientists*, March/April 2000.

⁵⁷ "With respect to allegations of industrial espionage, the notion that we collect intelligence to promote American business interests is simply wrong. We do not to [sic] target foreign companies to support American business interests." Federal News Service, Prepared Testimony of George J. Tenet, Director of Central Intelligence Before the House Committee on Intelligence, April 12, 2000, p. 4.

⁵⁸ Federal News Service, Hearing of the House Permanent Select Committee on Intelligence, April 12, 2000, p. 33.

⁵⁹ There is no provision in U.S. law for foreign intelligence agencies to assist U.S. firms and (continued...)

Woolsey has maintained that U.S. intelligence agencies do not collect information about foreign technology because American technology is, in general, far superior. There is, however, he argues, a real need to seek information about corrupt practices by foreign competitors and activities such as transfers of dual-use technologies for use in production of weapons of mass destruction as well as activities in countries subject to U.N. sanctions.⁶⁰

Some foreign observers continue to dispute U.S. claims and they will not easily be persuaded that their concerns are ill-founded. Suggestions of NSA electronic eavesdropping have clearly had resonance among members of the European Parliament which voted on July 5, 2000 to undertake a lengthy investigation of Echelon. The investigation will not include the calling of witnesses and, interestingly, an amendment calling for an investigation of eavesdropping by all EU governments was not adopted.⁶¹ In part, foreign objections stem from concern about the capabilities of NSA to monitor their communications and those of European companies. There is also, especially among some, irritation that the United States has a closer sigint relationship with some of its allies than with others. In part, however, observers perceive attacks on NSA's activities as instinctive hostility among political elements long skeptical of close U.S.-European relations and determined to forge a more independent European identity. Some objections also undoubtedly arise from deep-seated opposition to the work of all intelligence agencies.

There is no question that the worldwide capabilities of NSA cause suspicion and resentment among some foreign elements. U.S. officials justify NSA's activities on international law, the necessity to acquire information about threats to national security, international terrorism, and the narcotics trade. While the potential for abuse is acknowledged, the United States has a legal structure that regulates electronic surveillance. In addition, intelligence derived from sigint supports many collective military and diplomatic efforts with European and other allies.

⁵⁹ (...continued)

there are important privacy protections mandated by FISA. On the other hand, Article 8 of the European Convention on Human Rights recognizes a right of privacy that is not to be interfered with except as is necessary in "the interests of national security, public safety or the *economic well-being* of the country." (Emphasis added.) The full implications of this provision are uncertain, but it would not necessarily preclude the interception of communications by intelligence agencies to obtain commercial advantages for their country's businesses.

⁶⁰ R. James Woolsey, "Why We Spy on Our Allies," *Wall Street Journal*, March 17, 2000.

⁶¹ Ambrose Evans-Pritchard, "GCHQ Faces Inquiry over US 'Spying' on Europe," *Electronic Telegraph*, July 6, 2000.